**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Currently Amended) A validation protocol for determining authenticity of a printer consumable, said protocol including the steps of:

providing a printer containing a first authentication chip and a printer consumable containing a second authentication chip;

generating a secret random number and calculating a signature for the secret random number using a signature function, in the first chip, the first chip having a random function to produce random numbers from a seed, and the function advances after each successful validation, so that the next random number is produced from a new seed;

encrypting the secret random number and the signature by a symmetric encryption function using a first key, in the first chip;

passing the encrypted secret random number and signature from the first chip to the second chip;

decrypting the encrypted secret random number and signature with a symmetric decryption function using the first key, in the second chip;

calculating a signature for the decrypted secret random number using the signature function, in the second chip;

comparing the signature calculated in the second chip with the signature decrypted, in the second chip;

in the event that the two signatures match, in the second chip, encrypting the decrypted secret random number and a memory vector of the second chip by the symmetric encryption function using a second key to produce a first number and sending the memory vector and the first number to the first chip, the memory vector being comprised of variables holding updatable consumable state data of the printer consumable, the manner of updating the updatable consumable state data being protected by requiring clearing of the memory vector when access to change the updating manner is attempted;

calling a test function in the first chip by the first chip first receiving the memory vector and the first number from the second chip, the test function including:

encrypting the secret random number and the received memory vector by the symmetric encryption function using the second key, in the first chip, to produce a second number;

comparing the second number with the first number, in the first chip,

in the event that the comparison returns a match, considering the second chip to be valid and authorizing use of the printer consumable; and

in the event that the comparison returns a mismatch, considering the second chip to be invalid and denying use of the printer consumable.

2. (Previously Presented) The protocol according to claim 1, where the first and second keys are held in both the first and second authentication chips, and are kept secret.

3. (Cancelled)

4. (Previously Presented) The protocol according to claim 1, where the symmetric decrypt function is held only in the second chip.

5. (Previously Presented) The protocol according to claim 1, where the signature function generates digital signatures of 160 bits.

6. (Cancelled)

7. (Previously Presented) The protocol according to claim 6, where the time taken to return an indication the second chip is invalid is the same for all bad inputs, and the time taken to return the secret random number encrypted with the second key is the same for all good inputs.

8. (Previously Presented) The protocol according to claim 1, where a test function is held only in the first chip to advance the secret random number if the second chip is valid; otherwise it returns an indication the second chip is invalid.

9. (Previously Presented) The protocol according to claim 8, where the time taken to return an indication the second chip is invalid is the same for all bad inputs, and the time taken to return an indication the second chip is valid is the same for all good inputs.

10. (Original) The protocol according to claim 1, where it is used to determine the physical presence of a valid authentication chip.

11-20. (Cancelled)